MSL

MOORE STEPHENS LOVELACE CPAs & ADVISORS

Fraud Detection And Awareness

Presented By
William Blend, CPA, CFE

Agenda

- General Fraud Discussion
- Fraud Triangle and More
- Data from 2016 ACFE Report to the Nations
- Anatomy of an Investment Fraud
- Investments and Audits
- Controls are the Key
- Investment Red Flags

General Fraud Discussion

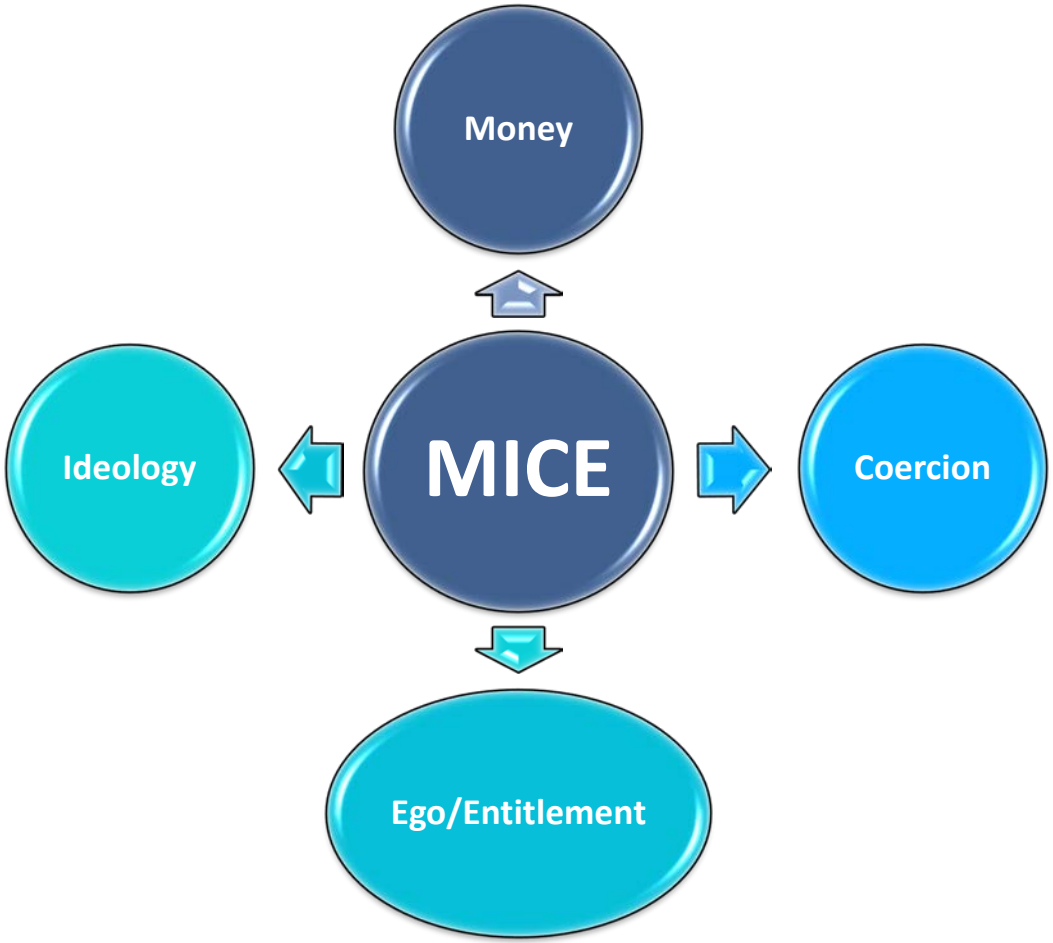
Ethics Relationship to Fraud

Ethics is a discipline dealing with what is good and bad with moral duty and obligation.

Fraud Triangle and More

Fraud Triangle…

Fraud Motivation



The Fraud Diamond – Considers Two Types of Fraudsters

Fraudsters – More Details

Accidental Fraudster

- Focus of Fraud Triangle
- First-Time Offender
- Well-Educated, Male, Middle-Class, Good Person
- Pressure Occurs
- Rationalization

Predator Fraudster

- Deliberate, Arrogant
- Seeks Opportunities
- No Pressure or Rationalization
- May Begin as Accidental
- Criminal Mindset

Fraud, Waste and Abuse

Fraud – an illegal act involving the obtaining of something of value through **willful** misrepresentation. **Fraud is a determination to be made through the judicial process.**

Waste – involves **not receiving reasonable value** for money in connection with any government-funded activities.

Abuse – involves **behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances**.

Computer Fraud

Computer fraud - the act of using computers, the Internet, Internet devices, and Internet services to defraud

- Computer fraud can allow for more fraud to occur in less time and with less effort
- Computer fraud often leaves little or no evidence making it more difficult to detect

Computer Fraud *(Cont.)*

What is good about computers is also what makes them more vulnerable

- Databases are large and access privileges can be difficult to create and enforce, making theft, destruction or altering of data easier and quicker
- The desire to allow employees, customers, and vendors access to an organization's system also creates more exposure
- Once a system is altered or accessed, it remains that way until the system is no longer used or the breach is discovered

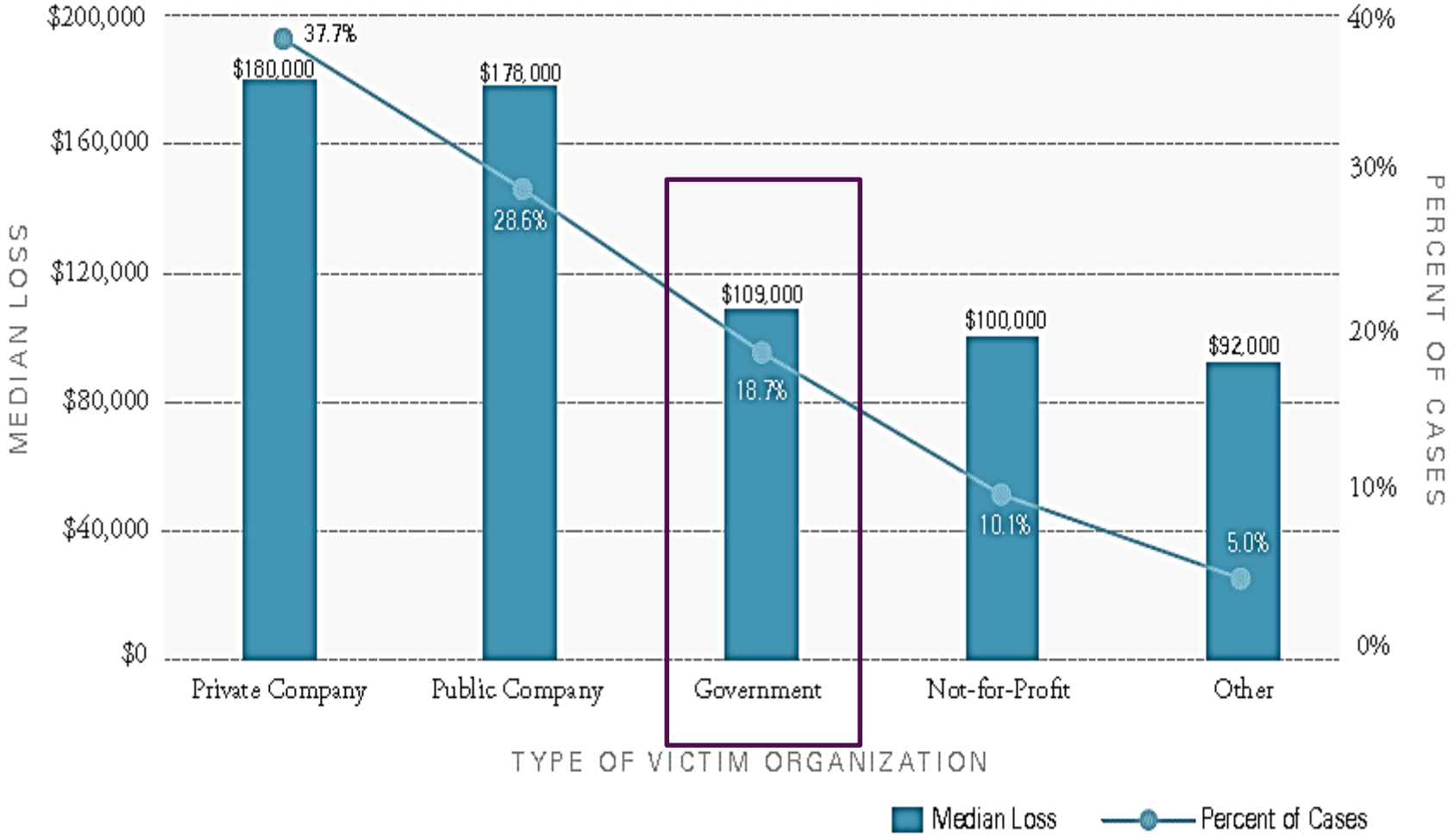
Computer Fraud *(Cont.)*

Classifications of Computer Fraud include:

- Input Fraud – alteration or falsifying of data input
- Processor Fraud – unauthorized system use
- Computer Instructions Fraud – modifying, illegal copying, or misuse of software
- Data Fraud – illegal copying, using, browsing, searching, or harming data
- Output Fraud – stealing, copying, or misusing computer printouts or displayed information

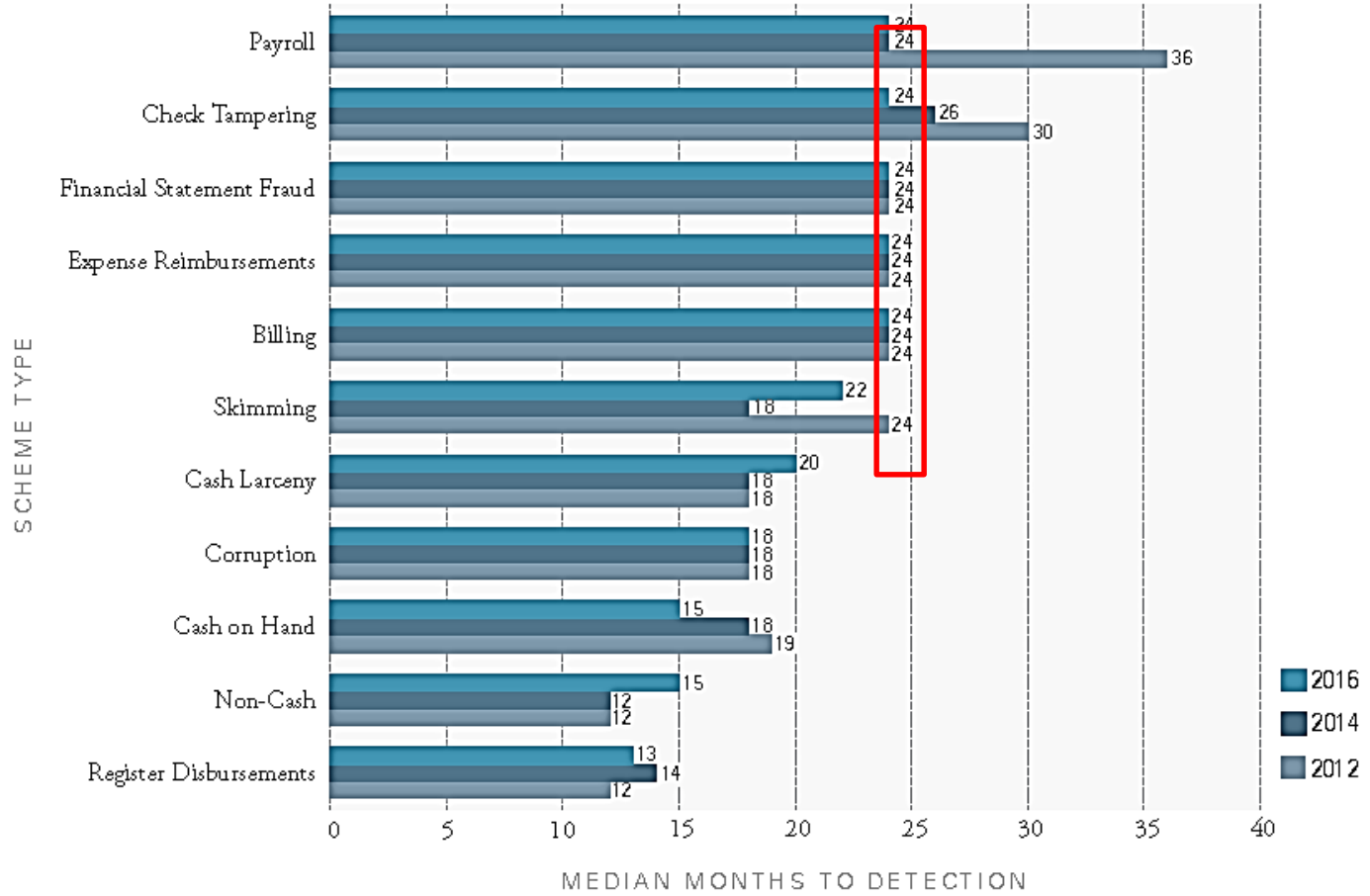
Data – From 2016 ACFE Report to the Nations

Victim Organizations - Government



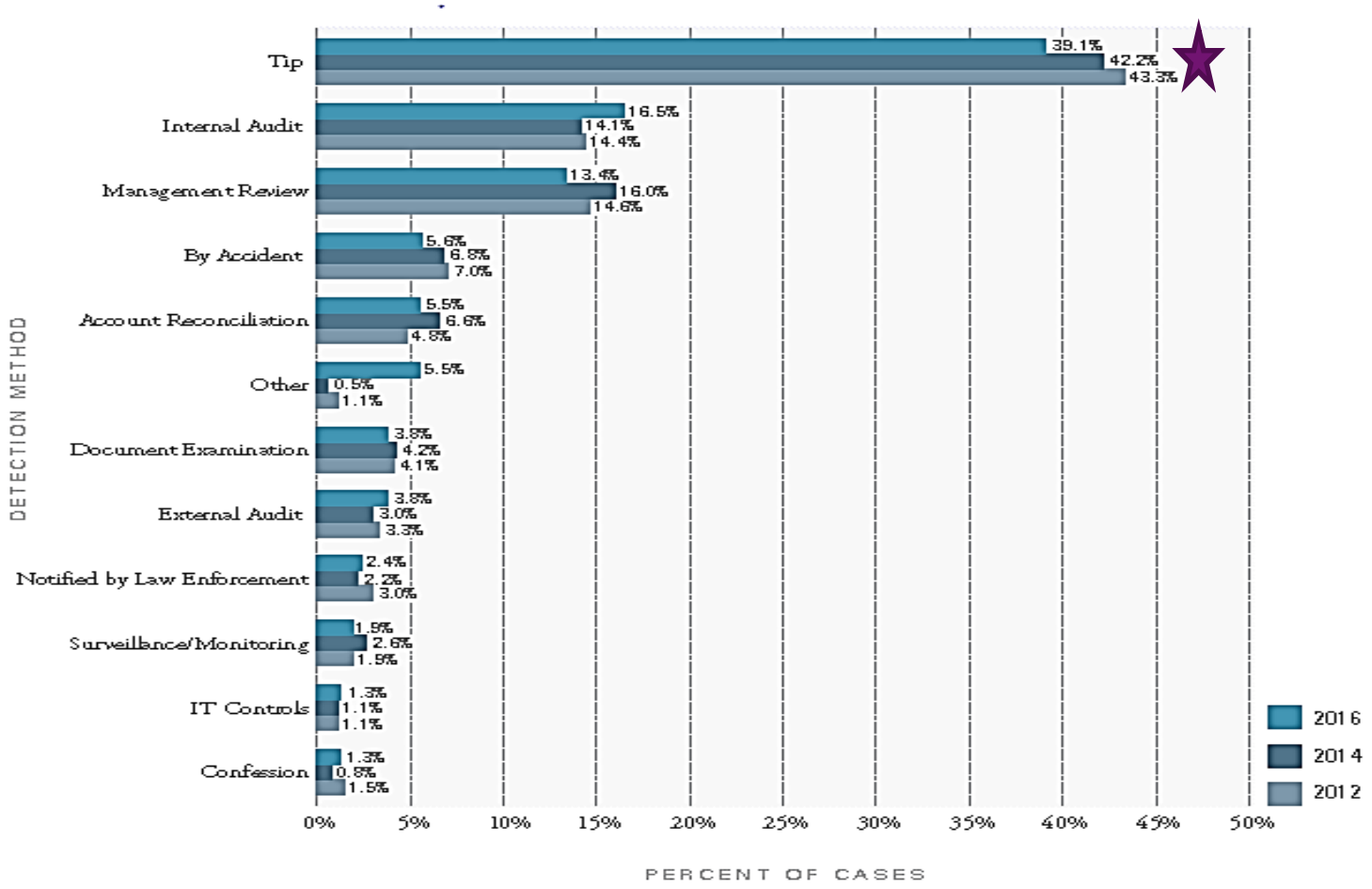
How Occupational Fraud is Committed

Duration of Fraud Based on Scheme Type



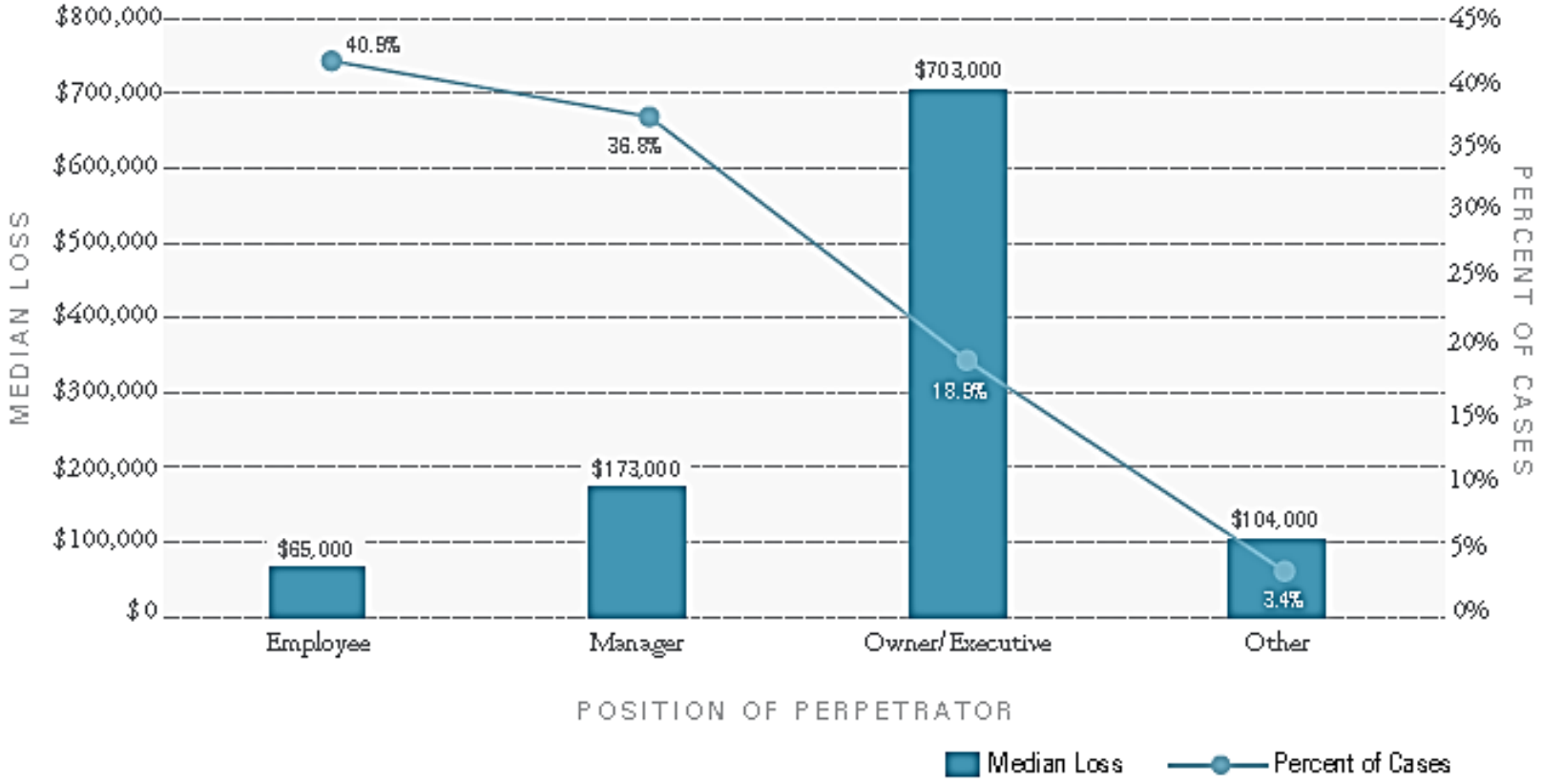
Detection of Fraud Schemes

Initial Detection of Occupational Frauds



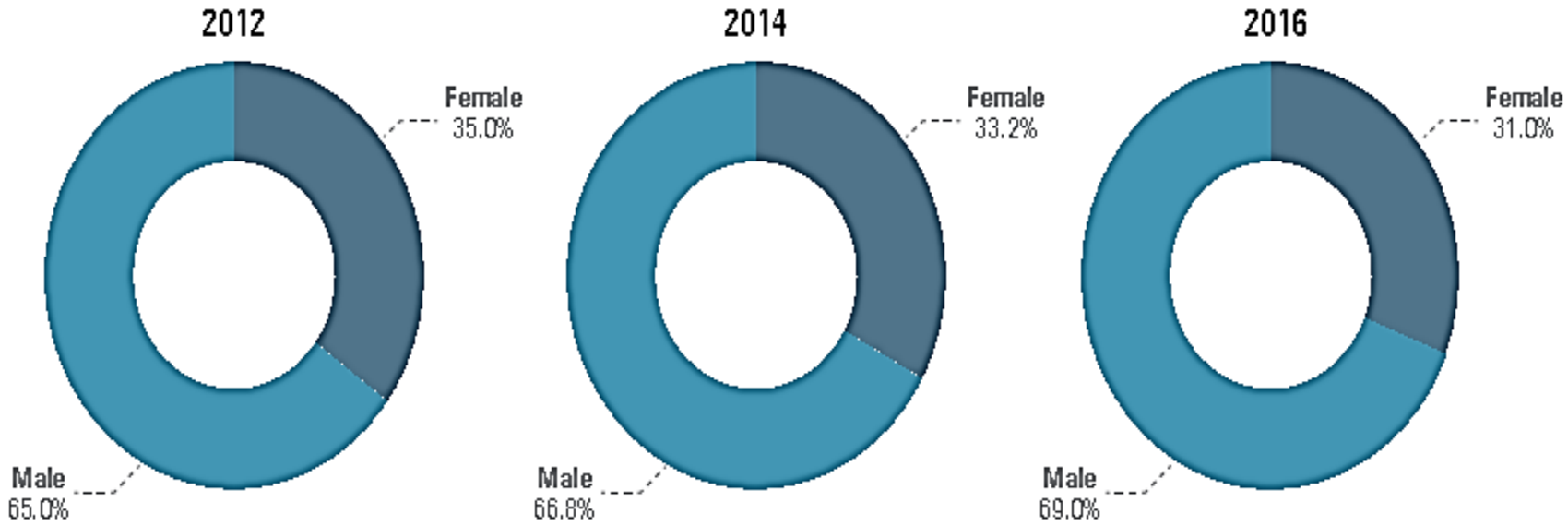
Perpetrators

Position of Perpetrator — Frequency and Median Loss



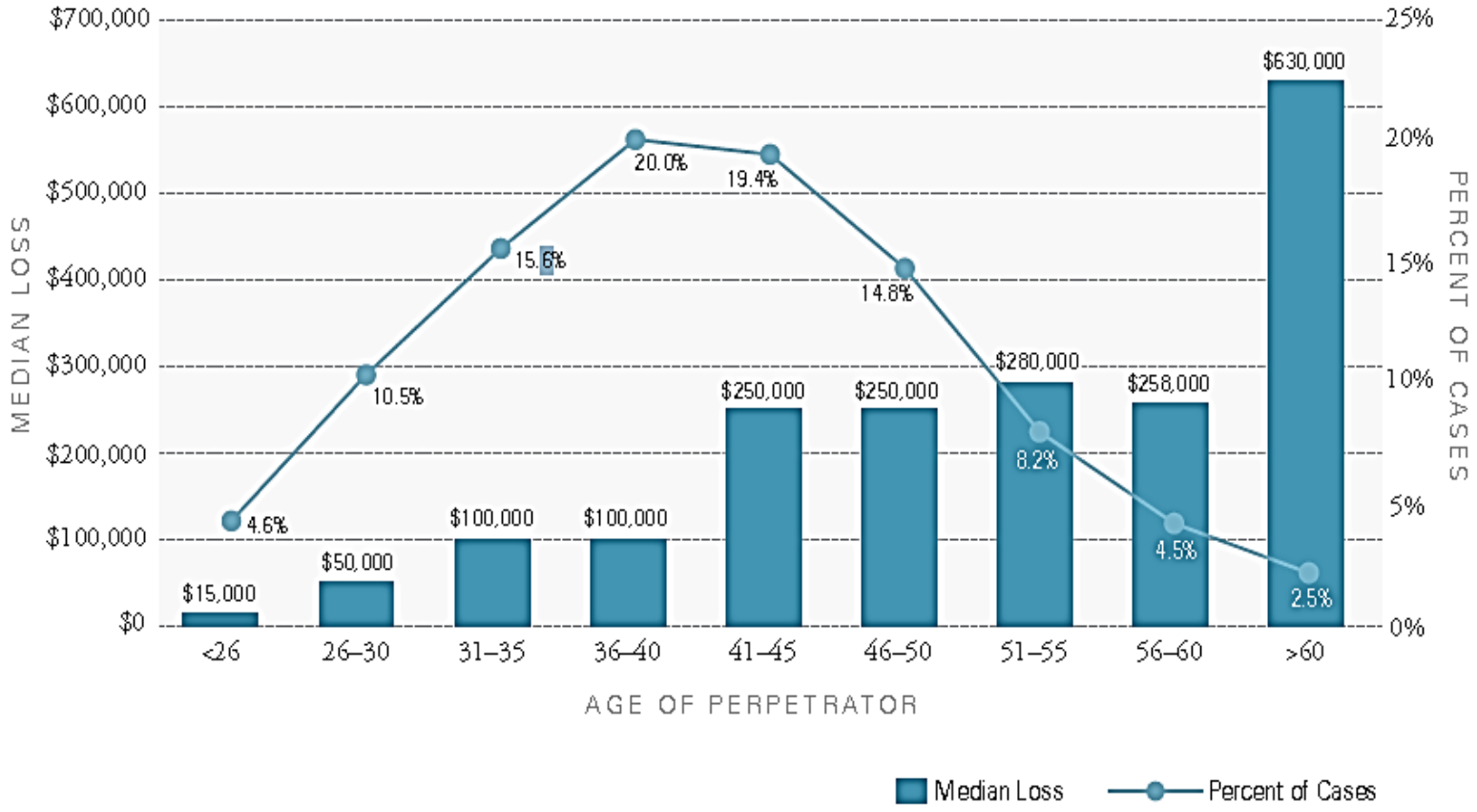
Perpetrators *(Cont.)*

Gender of Perpetrator — Frequency



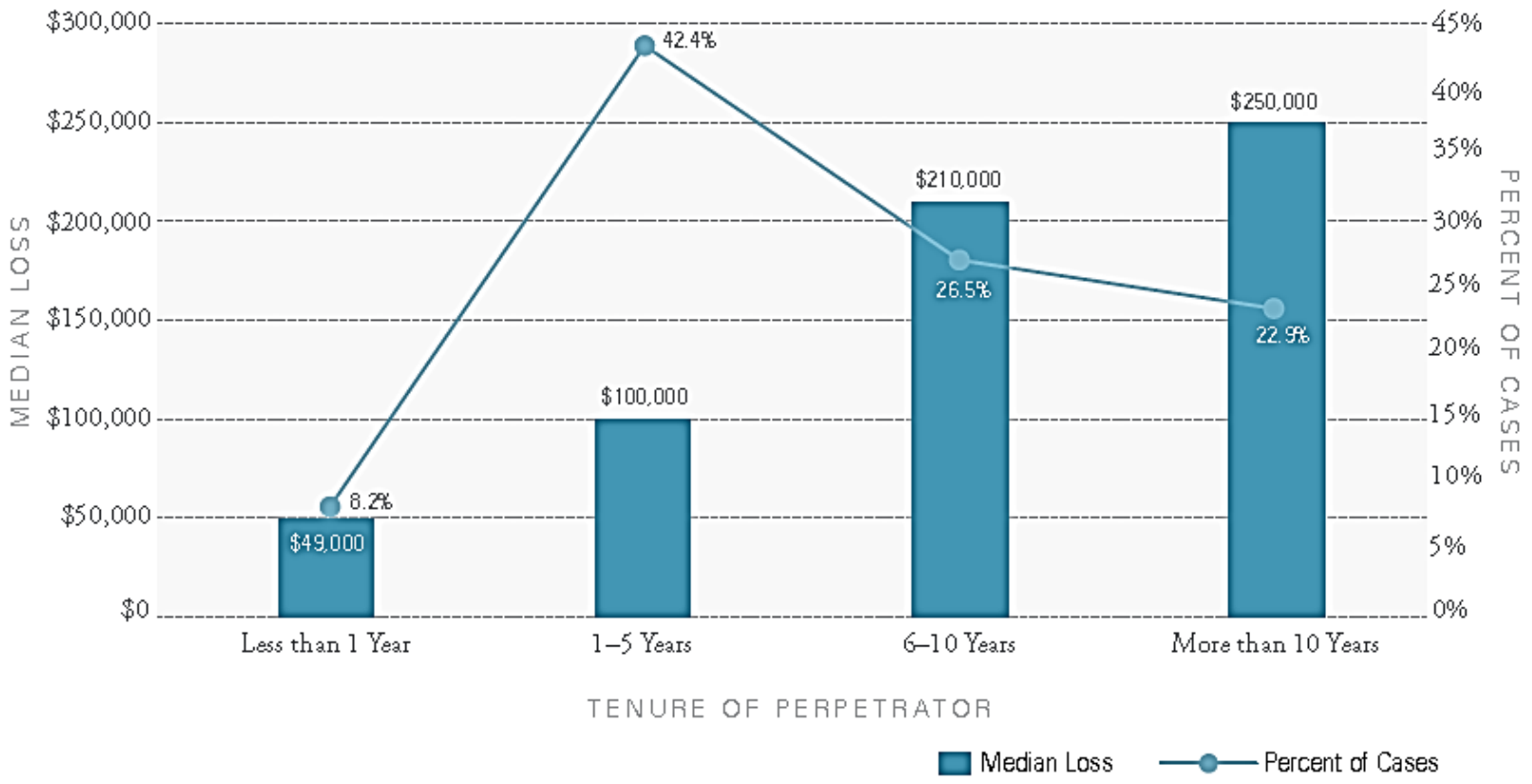
Perpetrators *(Cont.)*

Age of Perpetrator — Frequency and Median Loss



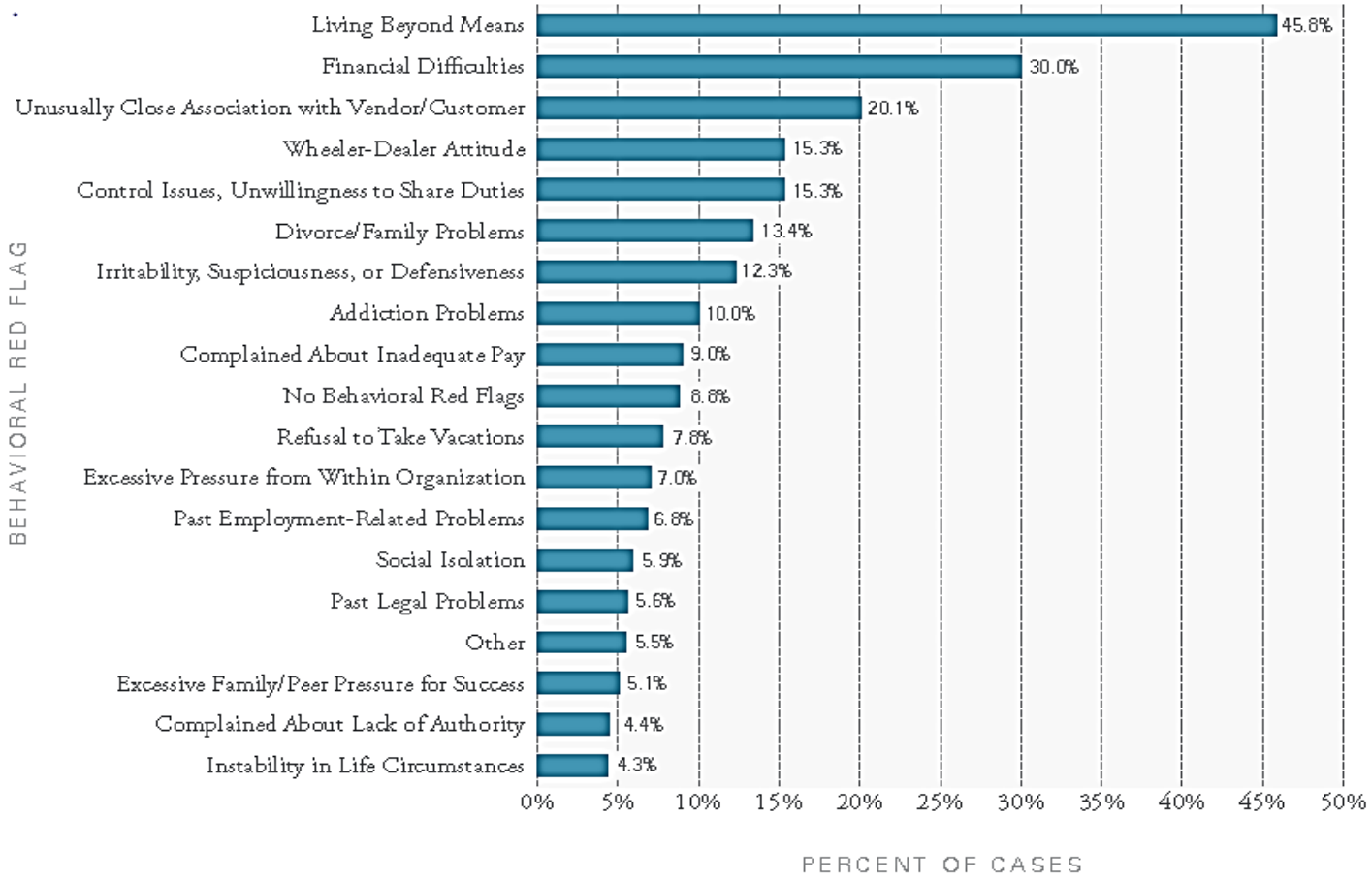
Perpetrators *(Cont.)*

Tenure of Perpetrator — Frequency and Median Loss



Perpetrators *(Cont.)*

Behavioral Red Flags of Perpetrators



Anatomy of an Investment Fraud

Investment Fraud

- Discussion

AUDITS IMPACTING INVESTMENTS

Audits

Financial Statement Audits – Focuses on looking for misstatements in the financial statements, does include a compliance component.

Internal Audits – Generally focuses on operational activities of an organization, but can involve both financial and forensic aspects

Forensic (Fraud) Audits – Focuses on identification of fraud. Usually, narrowly focuses on specific allegation or suspected fraudulent activity

Controls Are the Key

Types of Controls

Preventive

Detective

Corrective

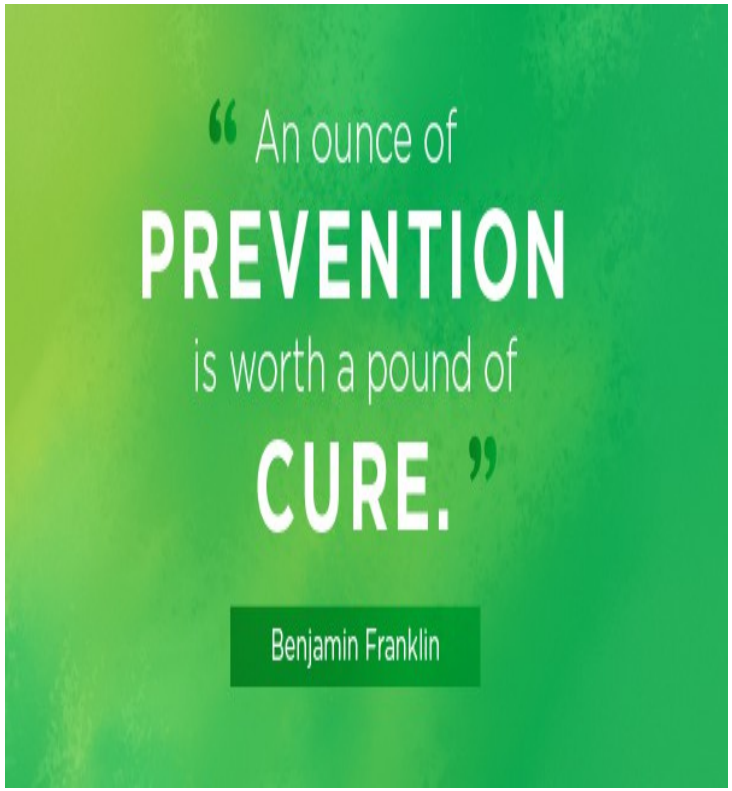
Manual and Automated

Types of Controls - Preventive

Preventive controls prevent problems before they arise

Examples:

- ✓ Approval, authorization, and verification of transactions
- ✓ Segregation of duties
- ✓ Securing assets



Types of Controls - Detective

Detective controls detect problems <u>that have occurred</u>

Examples:

- ✓ Performance reviews
- ✓ Reconciliations
- ✓ Internal audits

Types of Controls - Corrective

Corrective controls correct problems that have been detected

Examples:

- ✓ Policies and procedures
- ✓ Training programs
- ✓ Reconstruction of data
- ✓ Disciplinary action

IT Controls

IT Preventive Technical Controls

Preventive technical controls are used to **prevent unauthorized personnel or programs** from gaining remote access to computing resources. Examples include:

- Access control software
- Antivirus software
- Library control systems
- Passwords
- Smart cards
- Encryption
- Dial-up access control and callback systems

IT Preventive Administrative Controls

Preventive administrative controls are **personnel-oriented** techniques for controlling behavior, to ensure confidentiality, integrity, and availability of computing data. Examples include:

- Security awareness and technical training
- Separation of duties
- Procedures for recruiting and terminating employees
- Security policies and procedures
- Supervision
- Disaster recovery, contingency, and emergency plans
- User registration for computer access

IT Detective Technical Controls

Preventive technical controls **warn personnel of violations or attempted violations** of preventive technical controls. Examples include:

- Audit trails
- Intrusion detection

IT Detective Administrative Controls

Detective administrative controls are **used to determine how well security policies and procedures are complied with**, to detect fraud, and to avoid employing personnel who represent an unacceptable security risk. Examples include:

- Security reviews and audits
- Performance evaluations
- Required vacations
- Background investigations
- Rotation of duties

IT Controls – ACH and Wire Transfers

Best practices for using ACH and Wire Transfers:

- Written policies and procedures
- Debit Blocks – electronic debits are rejected before posting to your account
- Transaction Verification – files held in suspension until an authorized individual is able to validate item counts and amounts
- Regular reconciliation of transaction activity – this should be done at least monthly but with electronic banking can be done more frequently
- Check with your banking entity

IT Controls – Internet Transactions

Best practices for Internet transactions:

- Segregate responsibilities for entries and approvals
- Use dual controls (two people involved in each transaction; initiator and approver)
- Use multi-factor authentication tools (secure ID token, digital certificates, smart cards)
- Delete exiting employees' user and IDs and authorities
- Require password changes to be done periodically and have strong password requirements
- Always signoff your computer when leaving station

Investment Internal Controls

The COSO Framework

- Relationship of Objectives and Components
  - Direct relationship between objectives (which are what an entity strives to achieve) and the components (which represent what is needed to achieve the objectives)

- COSO depicts the relationship in the form of a cube:
  - The three objectives are represented by the columns
  - The five components are represented by the rows
  - The entity's organizational structure is represented by the third dimension

Source: COSO

Five Components of COSO IC Model

1. **Control Environment - sets the tone** influencing awareness of good controls, procedures, accountability, and program management. **It is the foundation for all other IC components.**

2. **Risk Assessment - identification and analysis of relevant risks** associated with achieving objectives, such as risk and performance goals. Forms the basis for determining how risks should be managed.

3. **Information and Communication - is needed by management and employees to monitor progress in meeting the organization's mission and objectives** while maintaining proper accountability and internal control.

Five Components of COSO IC Model
(Cont.)

4. **Control Activities - are the policies and procedures established to achieve set objectives.** They help ensure that management's directives are carried out in daily program operations.

5. **Monitoring - accomplished through routine, ongoing activities, separate evaluations, or both**. Internal control systems should be monitored to assess their effectiveness and to modify procedures, as appropriate, based on results of the monitoring activities (feedback).

Investment Internal Controls

General Controls

- Government should have a written investment policy that has been approved by the governing body.
- Policies should be reviewed and revised periodically. All changes should be approved by the governing body.
- Process of initiating, reviewing, and approving investment purchases and sales should be recorded and retained for audit purposes.

Investment Internal Controls *(Cont.)*

General Controls *(Cont.)*

- Written wire transfer agreement should outline controls and security provisions for making and receiving wire transfers.

- Written or electronic confirmations of telephone transactions for investments and wire transfers should be required.

- Segregation of duties, no one person should have responsibility for investment transactions from beginning to end.

Investment Internal Controls *(Cont.)*

General Controls *(Cont.)*

- Investment procedures should be fully documented, should include descriptions of employee responsibilities, the process for conducting and recording transactions, and outline the authority to approve the transactions.

- A formal training plan should be part of the investment policy. It should ensure that responsible parties obtain training to understand investment holdings.

- Monthly verification of both principal and market values of all investments and collateral should be obtained.

Investment Internal Controls *(Cont.)*

General Controls *(Cont.)*

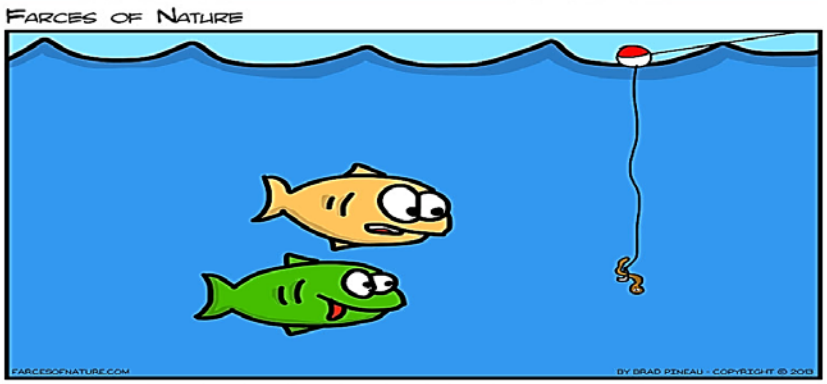
- Investment reporting should be performed on a periodic basis and presented to the governing body.
- Periodic internal control audits should be performed to verify that controls are functioning properly, are in compliance with investment policy and are updated for current operational structure.
- Consideration should be given to implementation of an investment committee and/or third-party financial advisor separate from broker/advisor. Function should include evaluation of fees, portfolio earnings and risk.

Investment Red Flags

Investment Red Flags

Promises of High Returns with Little or No Risk:

- Promise of a high rate of return, with little or no risk, is a classic warning sign of investment fraud.
- Every investment carries some degree of risk, and the potential for greater returns generally comes with greater risk.
- Avoid “can’t miss” investment opportunities or those promising “guaranteed returns.” Remember – if it sounds too good to be true, it probably is.



"GEEZ I DUNNO, NORM. IT SEEMS TOO GOOD TO BE TRUE."

Investment Red Flags *(Cont.)*

Unregistered Persons:

- Always ensure that investment advisors, brokers, etc., are registered, licensed, and insured. No licensed and registered persons often are involved with securities fraud.
- Search SEC's online database Investment Adviser Public Disclosure (IAPD)
- Search Financial Industry Regulatory Authority (FINRA)
- Contact state securities regulator

Investment Red Flags *(Cont.)*

Financial Professional Background:

- Employed at firms expelled from securities industry
- Personal bankruptcy
- Termination from previous employer(s)
- Subject to internal review at employer
- High number of customer complaints
- Failed industry qualification examinations
- Federal tax liens
- Repeatedly moving firms

Investment Red Flags *(Cont.)*

Portfolio/Account Activity:

- Excessive trading, if pervasive, may be a strong indicator of churning
- Over-concentration of allowable investment types
- Over/under performance
- Overly consistent performance
- Account discrepancies – unauthorized trades, missing funds, statement errors
- Resistance to third-party oversight of performance

Questions or Comments